



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/574,345	05/19/2000	Derek C. Au	28189.00010	8281

25224 7590 09/30/2005

MORRISON & FOERSTER, LLP
555 WEST FIFTH STREET
SUITE 3500
LOS ANGELES, CA 90013-1024

EXAMINER

SHIN, KYUNG H

ART UNIT	PAPER NUMBER
----------	--------------

2143

DATE MAILED: 09/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/574,345

Applicant(s)

AU ET AL.

Examiner

Kyung H. Shin

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2 and 4-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2 and 4-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

20

DETAILED ACTION

Response to Amendment

1. In view of the Appeal Brief filed on 7/15/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. Claims **1, 2, 4 - 16** are pending. **Claims 3, 17 - 22** have been cancelled; **Claims 1, 2, 4 - 10, 15** have been amended on 6/28/2004 after Non-Final action. Independent claims are **1, 10, 15**.

Claim Rejections - 35 USC § 103

The text of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. **Claims 1, 2, 4 - 16** are rejected under 35 U.S.C.103(e) as being unpatentable over Jones (U.S. Patent No. 5,412,730) in view of Lynn (U.S. Patent No. 5,345,508) and further in view of DeBellis (US Patent No. 6,044,388) and further in view of Dent (U.S. Patent No. 5,060,266).

Regarding Claim 1, Jones discloses a pseudo-random key generator for use within a cryptographic communication system, said pseudo-random key generator comprising:
(see Jones Fig. 1 and Fig. 4)

- a) a pseudo-random number generator for periodically generating a plurality of pseudo-random numbers, wherein a pseudo-random number is generated for every occurrence of a predetermined key change period;
(see Jones col. 3, line 27: generate a new key based on pseudo-random values)
- b) a computer readable storage medium connected to said pseudo-random number generator. (see Jones col. 4, line 40, and col. 9, line 53)
- c) Jones does not disclose a timing circuit coupled to pseudo-random generator and a timing source to provide current timing values. However, Dent discloses a timing circuit operatively coupled to said pseudo-random number generator, said timing circuit includes a time/key initialization device and a timing source for providing current timing values, and (see Dent col. 11, line 21)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to utilize a timing circuit in the computation of a offset value for pseudo random generator update as taught by Dent. One of ordinary skill in the art would be motivated to employ Dent in order to optimize the implementation of a widely used and available secure encryption and synchronization technique between timing entities for network based encryption. (see Dent col. 2, lines 45-54: " ... agree on a secret mechanism for enciphering (encrypting) and deciphering (decrypting) the information ... use a particular encryption device which may be widely available, but which can be programmed with a secret key specific to the sender and receiver ... ")

- d) Jones does not disclose the usage of predetermined base value to compute the difference in timing values between two pseudo-random generators and to update pseudo-random generator for synchronization. However, Lynn and DeBellis disclose wherein, upon initialization of the pseudo-random key generator, said timing source compares a current timing value with a predetermined crypto midnight initialization timing value, and transmits the difference to the time/key initialization device, which causes the pseudo-random number generator to generate a set of initialization pseudo-random numbers starting from the crypto midnight initialization timing value a pseudo-random number is generated in sequence for all of the key change periods between the crypto midnight

initialization timing value and the current timing value. (see Lynn col. 2, lines 61-67; col. 3, lines 48-53: update pseudo-random generator utilizing base values ; see DeBellis col. 4, line 66 - col. 5, line 5: utilization of identical base values (i.e. secret values, time dependent value) results in identical generated keys, time dependent value (i.e. current time), secret value (i.e. crypto-midnight value), updated secret value (i.e. time period updated value))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to utilize base values in the computation of a timing offset to update pseudo random generator as taught by Lynn, and to modify Jones to utilize a base value in conjunction with a time dependent value as taught by DeBellis. One of ordinary skill in the art would be motivated to employ Lynn in order to optimize synchronization between timing entities in the performance of network based encryption techniques (see Lynn col. 2, lines 47-51: “ ... a high speed cryptosystem ... self synchronization between transmitter and receiver such that no additional recovery procedures are required ... ”), and to employ DeBellis in order to optimize the initialization function and strength of a pseudorandom number generator (see DeBellis col. 4, lines 36-39: “ ... a pseudorandom number generator that can be implemented on a single silicon chip, can be initialized with integrity, has a suitably high work factor, and has an algorithm simple enough, yet strong enough, that it can be published ... ”).

Art Unit: 2143

Regarding Claim 2, Jones does not explicitly disclose “time clock” to supply input of pseudo-random number generator although “block counter” was indicated. However, Dent in analogous art discloses “a time clock” (see Dent Fig. 5, numeral 201) to generate a count in response to an increment applied at the input, and generates a plurality of pseudo-random key stream bits.

Dent discloses the pseudo-random key generator according to claim 1, wherein said timing circuit (see Dent Fig. 5, numeral 201) further includes a delta counter operatively coupled to said time/key initialization device. (see Dent col. 11, line 21)

It would have been obvious to those of ordinary skill in the art at the time the invention was made to include therein “a time clock” (see Dent col. 11, line 60) generating input to the pseudo-random key generator of Jones as taught in Dent. One of ordinary skill in the art would have been motivated to use “a time clock” (see Dent Fig. 5, numeral 201) for the seed values of pseudo-random key generator in order to perform synchronization for efficient cryptographic communication.

Regarding Claims 4, 5, and 6, Jones discloses the pseudo-random key generator according to claim 1, wherein said computer readable storage (see Jones Fig. 4, col. 8, line 7) medium includes a PRN re-map table (see Jones col. 10, lines 6-9), a key block formation table. (see Jones col. 10, line 46) and timing circuit (see Jones Fig. 4, numeral 21).

Regarding Claim 7, Jones does not disclose a crypto midnight value and a key change

Art Unit: 2143

period value (base values to computer timing offset). However, Lynn and DeBellis discloses the pseudo-random generator according to claim 6, wherein said read only computer readable storage medium includes:

- a) the crypto midnight initialization timing value; (see Lynn col. 2, lines 61-67: base value to computer timing offset) (see DeBellis col. 4, line 66 - col. 5, line 5: utilization of identical base values (i.e. secret values, time dependent value) results in identical generated keys, time dependent value (i.e. current time), secret value (i.e. crypto-midnight value), updated secret value (i.e. time period updated value)) and
- b) the key change period value. (see Lynn col. 2, lines 61-67: base value for update) (see DeBellis col. 4, line 66 - col. 5, line 5: utilization of base values (i.e. secret values, time dependent value) results in identical generated keys, secret value (i.e. crypto-midnight value), updated secret value (i.e. time period updated value))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to utilize base values in the computation of a timing offset to update pseudo random generator as taught by Lynn, and to modify Jones to utilize a base value in conjunction with a time dependent value as taught by DeBellis. One of ordinary skill in the art would be motivated to employ Lynn in order to optimize synchronization between timing entities in the performance of network based encryption techniques (see Lynn col. 2, lines 47-

51), and to employ DeBellis in order to optimize the initialization function and strength of a pseudorandom number generator (see DeBellis col. 4, lines 36-39)

Regarding Claim 8, Jones discloses the pseudo-random key generator according to claim 6, wherein said computer readable storage medium includes an executable program, (see Jones col. 11, lines 11-18) causing said systems re-map generator to re-map the data of PRN re-map table. (see Jones col. 2, lines 8-24)

Regarding Claim 9, Jones discloses the pseudo-random key generator according to claim 8, wherein said systems re-map generator selectively rearranges data stored in said computer readable storage medium. (see Jones col. 10, lines 21-29)

Regarding Claim 10, Jones discloses a cryptographic communication system having a pseudo-random key generator (see Jones Fig. 4, numeral 23) for generating cryptographic keys, said pseudo-random key generator comprising:

- a) a pseudo-random number generator, (see Jones Fig. 4, numeral 38)
- b) a timing circuit operatively coupled to said pseudo-random number generator; (see Jones Fig. 4, numeral 21)
- c) a first computer readable storage area operatively coupled to said pseudo-random number generator, said first computer readable storage area containing a plurality of data values, each data value associated with a unique storage address within said first computer readable storage area: (see Jones col. 4, lines 35-43)

- d) a second computer readable storage area operatively coupled to said first computer readable storage area, said second computer readable storage area containing a plurality of key data values, each key data value associated with a unique storage address within said second computer readable storage area, (see Jones col. 9, lines 55-60)
- e) wherein the pseudo-random number generator periodically generates a pseudo-random number in accordance with the timing circuit, wherein each generated pseudo-random number is used to look up a unique address in the first computer readable storage area for retrieving the data value associated with the looked up unique address, and wherein the retrieved data value is used to look up a unique address in the second computer readable storage area for retrieving a key value data, said key value data being used to form a cryptographic key. (see Jones col. 9, lines 51-62)

Lynn and DeBellis disclose:

- f) wherein, upon initialization of the pseudo-random key generator, said timing circuit compares a current timing value with a predetermined crypto midnight initialization timing value and cause the pseudo-random number generator to generate a set of initialization pseudo-random numbers starting from the crypto midnight initialization timing value until a pseudo-random number is generated in sequence for all of the key change periods

between the crypto midnight initialization timing value and the current timing value. (see Lynn col. 2, lines 61-67; col. 3, lines 48-53: update pseudo-random generator utilizing base values ; see DeBellis col. 4, line 66 - col. 5, line 5: utilization of identical base values (i.e. secret values, time dependent value) results in identical generated keys, time dependent value (i.e. current time), secret value (i.e. crypto-midnight value), updated secret value (i.e. time period updated value))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to utilize base values in the computation of a timing offset to update pseudo random generator as taught by Lynn, and to modify Jones to utilize a base value in conjunction with a time dependent value as taught by DeBellis. One of ordinary skill in the art would be motivated to employ Lynn in order to optimize synchronization between timing entities in the performance of network based encryption techniques. (see Lynn col. 2, lines 47-51), and to employ DeBellis in order to optimize the initialization function and strength of a pseudorandom number generator (see DeBellis col. 4, lines 36-39)

Regarding Claim 11 and 13, Jones discloses the cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said first/second computer readable storage area for generating the data values in accordance with a predetermined algorithm. (see Jones col. 10, lines 61-65)

Art Unit: 2143

Regarding Claim 12, 14 and 16, Jones discloses the cryptographic communication system according to claim 11, wherein said programmed processor selectively rearranges the data values in said first/second computer readable storage area. (see Jones col. 10, line 66 - col. 11, line 8)

Regarding Claim 15 (currently amended), Jones discloses a method of generating cryptographic keys using a pseudo-random number generator, a first/second computer readable storage area, said method comprising the steps of:

- a) inputting into said pseudo-random number generator an initial data value;
(see Jones col. 3, lines 26-33)
- d) generating a first data string by using said generated current time pseudo-random numerical value to look up a unique memory address in the first computer readable storage area (see Jones col. 10, line 7) and retrieving a data value associated with the unique memory address in the first compute readable storage area, said data value being one of a plurality of data values stored in the first computer readable storage area; and (see Jones col. 9, lines 29-44)
- e) generating a second data string by using said first data string to look up a unique memory address in the second computer readable storage area (see Jones col. 10, line 7) and retrieving a key data value associated with the unique memory address in the second compute readable storage area, said key data value being one of a plurality of key data values stored

in the second computer readable storage area, (see Jones col. 9, lines 44-50)

- f) wherein the retrieved key data value is used to form a cryptographic key.
(see Jones col. 2, lines 8-24)

Jones does not disclose base values to determine a timing value offset for pseudo-random generator update. However, Lynn and DeBellis disclose:

- b) initializing said pseudo-random number generator, said step of initialization includes steps of determining a difference between a crypto midnight initialization time value and a current time value, and causing said pseudo-random number generator to generate a set of initial pseudo-random numerical values; (see Lynn col. 2, lines 61-67; col. 3, lines 48-53: update pseudo-random generator utilizing base values; see DeBellis col. 4, line 66 - col. 5, line 5: utilization of identical base values (i.e. secret values, time dependent value) results in identical generated keys, time dependent value (i.e. current time), secret value (i.e. crypto-midnight value), updated secret value (i.e. time period updated value))
- c) generating a current time pseudo-random numerical value; (see Lynn col. 2, lines 61-67; col. 3, lines 48-53: update pseudo-random generator utilizing base values)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to utilize base values in the computation of a timing offset to update pseudo random generator as taught by Lynn, and to modify Jones to utilize a base value in conjunction with a time dependent value as taught by DeBellis. One of ordinary skill in the art would be motivated to employ Lynn in order to optimize synchronization between timing entities in the performance of network based encryption techniques (see Lynn col. 2, lines 47-51), and to employ DeBellis in order to optimize the initialization function and strength of a pseudorandom number generator (see DeBellis col. 4, lines 36-39).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
September 27, 2005


DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100